

**GOOGLE LLC'S
RESPONSE TO THE
COURT'S 10/27/22
ORDER TO SHOW
CAUSE (DKT. 784)**

**Redacted Version of
Document Sought to
be Sealed**

QUINN EMANUEL URQUHART & SULLIVAN, LLP

Diane M. Doolittle (CA Bar No. 142046)
dianedoolittle@quinnemanuel.com
Sara Jenkins (CA Bar No. 230097)
sarajenkins@quinnemanuel.com
555 Twin Dolphin Drive, 5th Floor
Redwood Shores, CA 94065
Telephone: (650) 801-5000
Facsimile: (650) 801-5100

Andrew H. Schapiro (admitted *pro hac vice*)
andrewschapiro@quinnemanuel.com
Teuta Fani (admitted *pro hac vice*)
teutafani@quinnemanuel.com
Joseph H. Margolies (admitted *pro hac vice*)
josephmargolies@quinnemanuel.com
191 N. Wacker Drive, Suite 2700
Chicago, IL 60606
Telephone: (312) 705-7400
Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)
stephenbroome@quinnemanuel.com
Viola Trebicka (CA Bar No. 269526)
violatrebicka@quinnemanuel.com
Crystal Nix-Hines (CA Bar No. 326971)
crystalnixhines@quinnemanuel.com
Alyssa G. Olson (CA Bar No. 305705)
alyolson@quinnemanuel.com
865 S. Figueroa Street, 10th Floor
Los Angeles, CA 90017
Telephone: (213) 443-3000
Facsimile: (213) 443-3100

Josef Ansorge (admitted *pro hac vice*)
josefansorge@quinnemanuel.com
Xi ("Tracy") Gao (CA Bar No. 326266)
tracygao@quinnemanuel.com
Carl Spilly (admitted *pro hac vice*)
carlspilly@quinnemanuel.com
1300 I Street NW, Suite 900
Washington D.C., 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100

Counsel for Defendant Google LLC
Additional counsel on signature pages

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, OAKLAND DIVISION

CHASOM BROWN, WILLIAM BYATT,
JEREMY DAVIS, CHRISTOPHER
CASTILLO, and MONIQUE TRUJILLO,
individually and on behalf of all similarly
situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 4:20-cv-03664-YGR-SVK

**GOOGLE LLC'S RESPONSE TO THE
COURT'S OCTOBER 27, 2022 ORDER
TO SHOW CAUSE (DKT. 784)**

Referral: Hon. Susan van Keulen, USMJ

San Jose Courthouse, Courtroom 6 – 4th Floor

Date: March 2, 2023

Time: 10:00 a.m.

TABLE OF CONTENTS

	<u>Page</u>
I. INTRODUCTION.....	1
II. BACKGROUND	2
A. The Court’s May 20, 2022 Order	2
B. Google Conducted a Thorough Investigation in Response to the Court’s May 20 Order	3
C. The Investigation Identified Additional Logs Containing Incognito- Detection Bits	4
1. Mr. Šrámek’s Investigation Identified [REDACTED] Additional Logs, But No Undisclosed Use of the Incognito-Detection Bits	4
2. Google’s Prior Investigation Did Not Identify the Additional Ads Logs Because the “Maybe_Chrome_Incognito” Bit Was Copied Automatically, Not Implemented Purposefully	6
3. Google’s Inability to Identify the Final [REDACTED] Log Earlier Is Justified.....	7
D. The Additional Logs Do Not Contain Accretive Material Information	7
1. [REDACTED] Logs	7
2. [REDACTED] Logs	8
3. [REDACTED] Logs	9
4. [REDACTED] Logs	10
5. [REDACTED] Logs	11
6. [REDACTED] Logs	11
7. [REDACTED] Log	12
III. ARGUMENT.....	12
A. The June Logs Do Not Contain Accretive Information	13
B. Google Should Not Be Further Sanctioned.....	13
1. Google Has Not Further Violated the Court’s Discovery Orders	14
2. Google’s Good-Faith Conduct Does Not Warrant Sanctions Under the Court’s Inherent Power.....	14
C. None of the Sanctions Plaintiffs Request Is Warranted Here	15
1. Plaintiffs Have Not Been Further Prejudiced.....	15
a. The June Logs Would Not Have Put Plaintiffs in a Better Position to Argue Google’s Liability	15
b. The June Logs Have No Bearing On Plaintiffs’ Alleged Damages.....	17

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

c.	The June Logs Provide No New Information Concerning Plaintiffs’ Ability to Identify Class Members or Entitlement to Class Certification	18
d.	The June Logs Would Not Have Further Changed the Course of Discovery.....	19
2.	Plaintiffs’ Requested Preclusion Sanctions Are Unwarranted and Unnecessary	20
a.	Excluding Reliance on Messrs. Šrámek and Harren	20
b.	Precluding Argument on Joining Authenticated and Unauthenticated Data.....	21
c.	Other Proposed Preclusion Sanctions	22
3.	Further Adverse Jury Instructions Are Unwarranted.....	22
4.	Shifting All Special Master Fees to Google Is Inappropriate Here.....	23
IV.	CONCLUSION.....	24

TABLE OF AUTHORITIES**Page****Cases**

<i>Apple Inc. v. Samsung Elecs. Co.</i> , 888 F. Supp. 2d 976 (N.D. Cal. 2012).....	23
<i>Best Label Co. v. Custom Label & Decal, LLC</i> , 2022 WL 1525301 (N.D. Cal. May 13, 2022)	23
<i>Chambers v. NASCO, Inc.</i> , 501 U.S. 32 (1991).....	14
<i>Fink v. Gomez</i> , 239 F.3d 989 (9th Cir. 2001).....	14
<i>First Fin. Sec., Inc., v. Freedom Equity Grp., LLC</i> , 2016 WL 5870218 (N.D. Cal. Oct. 7, 2016).....	24
<i>Goodyear Tire & Rubber Co. v. Haeger</i> , 137 S. Ct. 1178 (2017).....	14
<i>Luxul Tech. Inc. v. NectarLux, LLC</i> , 2016 WL 3345464 (N.D. Cal. June 16, 2016)	13
<i>Meta Platforms, Inc. v. BrandTotal Ltd.</i> , 2022 WL 1990225 (N.D. Cal. June 6, 2022)	23
<i>Natural-Immunogenics Corp. v. Newport Tr. Grp.</i> , 2016 WL 11520757 (C.D. Cal. June 16, 2016).....	20
<i>Network Appliance, Inc. v. Bluearc Corp.</i> , 2005 WL 1513099 (N.D. Cal. June 27, 2005)	20
<i>Nuance Comms., Inc. v. ABBYY Software House</i> , 2012 WL 5904709 (N.D. Cal. Nov. 26, 2012).....	21
<i>R&R Sails, Inc. v. Ins. Co. of Pa.</i> , 673 F.3d 1240 (9th Cir. 2012)	20
<i>Synapsis, LLC v. Evergreen Data Sys., Inc.</i> , 2006 WL 2884413 (N.D. Cal. Oct. 10, 2006).....	20
<i>Toth v. Trans World Airlines, Inc.</i> , 862 F.2d 1381 (9th Cir. 1988)	24
<i>True Health Chiropractic Inc. v. McKesson Corp.</i> , 2015 WL 5341592 (N.D. Cal. Sept. 12, 2015).....	20

Rules and Regulations

Fed. R. Civ. P. 37(b)(2)	23, 24
Fed. R. Civ. P. 37(e)(1).....	23
Fed. R. Civ. P. 37(e)(2).....	23

1 **I. INTRODUCTION**

2 Google hereby responds to the Court’s order to show cause in connection with Google’s
 3 June 14, 2022 identification of previously undisclosed logs (“June Logs”) containing the three
 4 “Incognito-detection bits.” On May 20, 2022, the Court sanctioned Google for not having earlier
 5 identified and disclosed the existence of the Incognito-detection bits and certain logs containing
 6 them, and ordered Google to confirm that no other logs contained those bits. Dkt. 588. After an
 7 extensive investigation, Google identified no use of the Incognito -detection bits that had not already
 8 been disclosed, litigated, and addressed by the Court’s May 20 order. Google’s investigation did
 9 uncover additional logs containing the Incognito-detection bits, and Google disclosed those logs
 10 immediately. The reason Google did not identify the June Logs at the same time it identified the
 11 earlier disclosed logs containing the Incognito-detection bits is that the bits were incorporated into
 12 the June Logs through automated processes that duplicated fields from earlier-disclosed logs,
 13 unbeknownst to the engineers Google consulted during its prior investigation.

14 The Court has asked Google to explain why the June Logs do not “contain relevant data that
 15 should have been identified and produced during discovery” and to show cause as to why Google
 16 should not be sanctioned for not discovering and disclosing them earlier. Dkt. 784. In particular, at
 17 the October 27, 2022 conference, the Court asked that Google support its position that the June Logs
 18 are non-accretive. This brief and accompanying evidentiary submissions show that the June Logs
 19 have no accretive relevance to this litigation, and that their disclosure after the close of discovery
 20 has not prejudiced Plaintiffs. None of the June Logs has any bearing on Plaintiffs’ efforts to prove
 21 liability, calculate damages, or identify class members. Indeed, the Incognito-detection bits in the
 22 June Logs were never intended or used to identify or analyze Incognito browsing—the engineers
 23 who manage the June Logs were not even *aware* they contained the Incognito-detection bits.

24 Because Google has not deprived Plaintiffs of accretive evidence, they have suffered no
 25 prejudice other than that for which the Court has already sanctioned Google. And the circumstances
 26 of Google’s identification and disclosure of the June Logs—following an extensive investigation
 27 conducted in a good-faith attempt to fully comply with the Court’s order—do not support a finding
 28

1 of bad faith. Accordingly, additional sanctions under Rule 37(b) or the Court’s inherent authority
2 are not warranted.

3 **II. BACKGROUND**

4 **A. The Court’s May 20, 2022 Order**

5 Earlier this year, Plaintiffs brought a motion for sanctions concerning three bits that certain
6 Google engineers had developed in an attempt to estimate aggregate Incognito traffic in Chrome
7 (“Incognito-detection bits”).¹ Dkt. 588, Ex. A (Findings of Fact and Conclusions of Law) (“FFCL”)
8 at 3. Plaintiffs alleged that Google belatedly identified the Incognito-detection bits, the data sources
9 containing those bits, and the names of certain individuals involved in their creation and use. Dkt.
10 429-1 at 1–2; Dkt. 510-1 at 1–2. Plaintiffs claimed that the delayed disclosures resulted in their “(1)
11 inability to obtain relevant documents; (2) inability to obtain relevant testimony; (3) impairment of
12 the Special Master process; (4) impairment of expert discovery; (5) Google’s spoliation of data; and
13 (6) impairment of Plaintiffs’ ability to rebut Google’s contentions.” FFCL ¶ 156.

14 The Court considered each of these arguments and, on May 20, 2022, granted in part and
15 denied in part Plaintiffs’ motion. Dkt. 588. The Court found that “the existence and use of three
16 Incognito-detection bits was relevant to both Plaintiffs’ claims and Google’s defenses,” FFCL at 29,
17 that “[t]he course of discovery may have been different, more focused, or focused on different issues
18 had Google complied with its discovery obligations,” and that “by withholding relevant discovery
19 focused on Google’s Incognito-detection bits, Google prejudiced Plaintiffs’ ability to fully address
20 the assertions by Google, its counsel, and its witnesses,” *id.* at 31–32.

21 To address these findings, the Court ordered that Google “may not object to or present
22 argument against the timing of the development and implementation of the three Incognito-detection
23 bits at issue or the fact that such bits were implemented,” or rely on testimony from four Google
24 engineers (Chris Liao, Bert Leung, Mandy Liu, and Quentin Fiard) who participated in the
25 development and use of the three bits. Dkt. 588 ¶¶ 2–3. And the Court determined that, should
26 Google’s delayed disclosure of the Incognito-detection bits become relevant to an issue before the

27
28 ¹ The “Incognito-detection bits” are “is_chrome_incognito,” “is_chrome_non_incognito_mode,” and
“maybe_chrome_incognito.” FFCL at 3.

1 jury, it would be appropriate to instruct that Google failed to disclose (i) the names of Google
2 employees responsible for developing those bits and (ii) data sources reflecting their use. *Id.* ¶ 5.

3 The Court declined to award further relief requested by Plaintiffs, including precluding
4 Google from making any argument about Incognito-detection bits for the rest of the case, instructing
5 the jury that Google had altered evidence, and requiring Google to pay all special master fees from
6 the start of discovery. *See* FFCL at 39–43. Finding that “[t]he reliability of using the Incognito-
7 detection bits to identify Incognito traffic, let alone specific Incognito users, is in dispute,” *id.* at 25,
8 the Court held that “Google is not excluded from arguing against the reliability of the three
9 Incognito-detection bits in identifying class members,” *id.* at 40.

10 The May 20, 2022 order directed Google to “provide Plaintiffs with a representation in
11 writing no later than May 31, 2022 that other than the logs identified thus far as containing
12 Incognito-detection bits, no other such logs exist.” Dkt. 588 at 6. Pursuant to its investigation up to
13 that time, Google had identified and disclosed █████ logs containing one or more of the Incognito-
14 detection bits. *See, e.g.*, Dkt. 614-3 (“5/31 Šrámek Decl.”).

15 **B. Google Conducted a Thorough Investigation in Response to the Court’s May**
16 **20 Order**

17 Google immediately began working to comply with the Court’s May 20 order. The next
18 business day, Martin Šrámek, the Privacy Working Group lead for Chrome, began a formal
19 investigation to confirm that Google had identified all instances of the Incognito-detection bits in
20 its logs. 5/31 Šrámek Decl. ¶ 5. Supported by a team of three other employees, Mr. Šrámek
21 conducted a comprehensive code search to identify any reference to the X-Client-Data header
22 present in Google source code. Dkt. 695-4 (“8/18 Šrámek Decl.”) ¶ 5. Based on the results of this
23 code search, Mr. Šrámek and his team surveyed █████ engineering teams responsible for code
24 referencing the X-Client-Data header, and conducted follow-up interviews with █████ teams. *Id.*
25 The investigation sought to identify *any* instances in which the absence of the X-Client-Data header
26 might be treated as indicative of Incognito browsing, including, but not limited to, the three
27 Incognito-detection bits. Dkt. 614-2 (“6/14 Šrámek Decl.”) ¶ 4. The investigation was labor-
28

1 intensive and—despite the diligent efforts of Mr. Šrámek and his team—required approximately
 2 three weeks to complete. *See id.*

3 On the Court’s May 31, 2022 deadline, Google provided Plaintiffs with a declaration from
 4 Mr. Šrámek reaffirming that the [REDACTED] data logs Google had previously disclosed were the only data
 5 sources that Mr. Šrámek then knew to contain the Incognito-detection bits. 5/31 Šrámek Decl. That
 6 declaration further described Mr. Šrámek’s thorough investigation process and explained that it
 7 would require two additional weeks to fully run its course. *Id.* ¶¶ 4–5. In submitting this declaration
 8 while the investigation continued, Google’s intention was not to disobey the Court’s order. To the
 9 contrary, it was Google’s intent to comply with the order by providing Plaintiffs with specific
 10 information known on May 31 while continuing the investigation and updating Plaintiffs upon
 11 completion. Plaintiffs neither objected to the May 31 declaration nor to Google’s commitment to
 12 complete its investigation before providing a final report. Trebicka Decl. ¶ 5. Mr. Šrámek’s
 13 investigation concluded within the expected two-week timeframe, and Google provided Plaintiffs
 14 with an updated declaration on June 14, 2022. 6/14 Šrámek Decl. ¶ 4.

15 **C. The Investigation Identified Additional Logs Containing Incognito-Detection**
 16 **Bits**

17 **1. Mr. Šrámek’s Investigation Identified [REDACTED] Additional Logs, But No**
 18 **Undisclosed Use of the Incognito-Detection Bits**

19 None of the [REDACTED] teams surveyed or interviewed during Mr. Šrámek’s extensive
 20 investigation—encompassing all owners of Google source code referencing the X-Client-Data
 21 header—identified any use of the X-Client-Data header to infer Incognito browsing beyond those
 22 now long-since disclosed: the [REDACTED] team’s long-defunct use of the “is_chrome_incognito” and
 23 “is_chrome_non_incognito_mode” bits, and the extensively litigated implementation of the
 24 “maybe_chrome_incognito” bit by Bert Leung and other engineers on the Google Ads team.
 25 11/29 Šrámek Decl. ¶ 6.

26 But Google went further in its investigation. As a confirmatory step conducted in parallel
 27 with the main investigation, Mr. Šrámek worked with a [REDACTED] Logs Technical Lead to attempt to
 28 identify any other log containing the Incognito-detection bits, whether or not any Google employees

1 were using those bits to infer Incognito traffic. *Id.* ¶ 5. Google developed a custom script designed
 2 to perform this confirmatory analysis. Harren Decl. ¶ 7. As Google has explained in prior filings,
 3 Google does not maintain a comprehensive list of fields in [REDACTED] logs. Instead, the custom script
 4 queried a table containing field names present in daily scans of a random [REDACTED] sample of
 5 [REDACTED] log traffic over the past [REDACTED].² *Id.* ¶¶ 7–8. Mr. Šrámek then used the results of that script
 6 to compile a list of previously undisclosed logs that were writing values for the Incognito-detection
 7 bits. 6/14 Šrámek Decl. ¶ 4. Mr. Šrámek further investigated why his survey of teams that may have
 8 been using those bits did not previously identify the logs, and determined that the Incognito-
 9 detection fields were automatically populated to those logs. *See* 6/14 Šrámek Decl. ¶ 5. These
 10 investigations did not identify any previously undisclosed use of the Incognito-detection bits.
 11 11/29 Šrámek Decl. ¶ 6.

12 On June 14, 2022, Google provided Plaintiffs with a supplemental declaration detailing the
 13 final results of Mr. Šrámek’s investigation. 6/14 Šrámek Decl. That declaration listed [REDACTED] logs
 14 containing the Incognito-detection bits that previous investigations did not identify: [REDACTED] logs
 15 containing the “maybe_chrome_incognito” bit and [REDACTED] [REDACTED] log containing the
 16 “is_chrome_non_incognito_mode” bit. As detailed below, the inclusion of the Incognito-detection
 17 bits in all of these logs was automated and unintentional—the bits were never intended or used to
 18 track Incognito traffic in those logs.

19 In responding to the Court’s order to show cause, Google further determined that one of the
 20 [REDACTED] logs disclosed in Mr. Šrámek’s June 14 declaration has a corresponding log with
 21 [REDACTED]

22 ² The same table could be queried to generate a list of fields present in the same [REDACTED] scan of log
 23 traffic for a given [REDACTED] log. As Google has explained to the Court and Special Master, counsel—along
 24 with the numerous Google engineers with log expertise who consulted on the issue—previously believed no
 25 method existed for even approximating the list of fields in a [REDACTED] log. *See* Dkt. 527-4 at 15; Dkt. 527-16
 26 at 253–54 (Ex. 35). It remains true that Google has no resource to produce a full list of fields in a given log,
 27 but Google now believes that a custom script like the one described above would likely have produced a
 28 longer list than what Google was able to produce earlier using the [REDACTED] tool. This new information
 is not material at this stage because the Court already sanctioned Google for not identifying the
 “maybe_chrome_incognito” bit in the previously disclosed lists of fields, and for not identifying all data
 sources containing Incognito-detection bits. *See* FFCL at 28 (“Google should have informed the Special
 Master and Plaintiffs of the [‘Incognito-detection bits’] existence when Google made its proposal to produce
 only the ‘largest 100 fields’ in [REDACTED] logs.”); *id.* at 21 (“[Google’s] declarant’s ‘informed understanding’
 could and should have included [logs containing the Incognito-detection bits].”).

1 authenticated data (also known as a [REDACTED] log”) that also contains the
 2 “maybe_chrome_incognito” bit. Kahlon Decl. ¶ 3. Google identified that log only upon specifically
 3 investigating [REDACTED] logs corresponding to the logs at issue. Because the
 4 “maybe_chrome_incognito” field was not intentionally populated in that log and was too
 5 infrequently populated to be captured in the [REDACTED] sample of [REDACTED] data Google queried in
 6 its confirmatory analysis, Mr. Šrámek’s investigation did not identify it. Google regrets the
 7 inadvertent omission, but its explanations concerning the other [REDACTED] logs at issue apply equally
 8 to this additional log.

9 **2. Google’s Prior Investigation Did Not Identify the Additional Ads Logs**
 10 **Because the “Maybe_Chrome_Incognito” Bit Was Copied**
 11 **Automatically, Not Implemented Purposefully**

12 Google’s earlier investigation into the Incognito-detection bits reasonably focused on
 13 Google’s use of those bits—*i.e.* whether and why engineers had chosen to implement the Incognito-
 14 detection bits in specific Google logs. Therefore, the prior investigation identified logs Google
 15 employees in the relevant areas knew to contain those bits. *See, e.g.,* Dkt. 527-6
 16 (Ansorge Decl.) ¶ 55. But the “maybe_chrome_incognito” bit was not intentionally implemented in
 17 any of the [REDACTED] ads logs first identified in June. Rather, Google’s backend infrastructure *automatically*
 18 *copied* thousands of fields implemented in the previously disclosed [REDACTED] (specifically,
 19 [REDACTED] and [REDACTED] into the [REDACTED] logs Mr. Šrámek
 20 identified in his June 14 declaration. 6/14 Šrámek Decl. ¶ 5; Kahlon Decl. ¶ 7; Liu Decl. ¶ 7; Maki
 21 Decl. ¶¶ 4, 8; Lee Decl. ¶¶ 13, 19. One of the fields was the “maybe_chrome_incognito” bit. *Id.*

22 Given how the “maybe_chrome_incognito” bit was included in the June Logs, a reasonable
 23 investigation could not have unearthed them. The identification of the June Logs resulted from
 24 Google’s extraordinary efforts to comply with the Court’s order. Google’s further investigation
 25 entailed a dedicated team that conducted a comprehensive search for all uses of X-Client-Data
 26 Header across all Google code, consulted every team connected to those uses, and then performed
 27 a confirmatory search for the Incognito-detection bits in [REDACTED] logs. *See* 6/14 Šrámek Decl. ¶ 4.
 28 Even then, no engineer surveyed reported *using* “maybe_chrome_incognito” for any purpose not

1 long-ago disclosed. 11/29 Šrámek Decl. ¶ 6. For this reason, Google’s earlier investigation during
 2 the briefing of Plaintiffs’ first sanctions motion did not identify (and could not have identified) the
 3 June Logs because it reasonably focused on the known implementation and use of the bits to
 4 approximate Incognito usage. Engineers who own or work closely with the June Logs have since
 5 confirmed that they are unaware of *any* use of the Incognito-detection bits in those logs for any
 6 Incognito-related analysis—or for any other purpose. Kahlon Decl. ¶¶ 7–8; Liu Decl. ¶¶ 7–8; Maki
 7 Decl. ¶¶ 4, 5, 10; Lee Decl. ¶¶ 13–14, 20. Given these circumstances, it is unsurprising that the June
 8 Logs were not identified earlier.

9 **3. Google’s Inability to Identify the Final [REDACTED] Log Earlier Is Justified**

10 Google identified [REDACTED] logs containing the “is_chrome_non_incognito_mode” bit in
 11 preparation for Dr. Caitlin Sadowski’s March 10, 2022 Rule 30(b)(6) deposition, and disclosed them
 12 to Plaintiffs at that deposition. *See* Dkt. 510-7. Google identified the [REDACTED] and final [REDACTED] log
 13 containing that bit only after the labor-intensive investigation described above. *See* 6/14 Sramek
 14 Decl. ¶ 4. The “is_chrome_non_incognito_mode” bit has not been used for *any purpose* since 2018.
 15 FFCL ¶ 132. The [REDACTED] team was likely unable to identify this final log because that log is designed
 16 to eventually replace (and duplicate the function of) one of the logs the [REDACTED] team did identify,
 17 but is not yet fully operational. Kuzniar Decl. ¶¶ 4–5. Moreover, the [REDACTED] log identified in June
 18 2022 contains no cookie identifiers that could link the contents of the field with named or
 19 pseudonymous users. Kuzniar Decl. ¶¶ 6–7; *id.* Ex. A.

20 **D. The Additional Logs Do Not Contain Accretive Material Information**

21 The June Logs fall into seven categories: [REDACTED]
 22 [REDACTED]
 23 [REDACTED]. *See generally* 6/14 Šrámek Decl. None of these logs provides new material information
 24 about the existence or use of the Incognito-detection bits.

25 **1. [REDACTED] Logs**

26 Two of the June Logs are [REDACTED] logs. Liu Decl. ¶ 5. Google uses
 27 [REDACTED] logs to [REDACTED]
 28 [REDACTED]. *Id.* ¶ 3. To accomplish this, the [REDACTED] logs [REDACTED]

1 [REDACTED]
 2 [REDACTED]
 3 [REDACTED].³ *Id.* ¶¶ 3–4. [REDACTED] experiments recorded in [REDACTED] logs might, for example, test how
 4 a different ad bidding strategy would affect the bidding result. *Id.*

5 The only event-level browsing data in these [REDACTED] logs (including the
 6 “maybe_chrome_incognito” field) is duplicated directly from the [REDACTED] logs. *Id.* ¶ 4; *see also*
 7 6/14 Šrámek Decl. ¶ 6. All of the additional data stored in these [REDACTED] logs is [REDACTED] data
 8 generated through the experiments described above; none of that data reflects any actual user data.⁴
 9 Liu Decl. ¶ 4. Moreover, the “maybe_chrome_incognito” field in these [REDACTED] logs has not been used
 10 to identify or analyze Incognito browsing. *Id.* ¶ 8. These [REDACTED] logs contain the
 11 “maybe_chrome_incognito” field only because they automatically populate with copies of all fields
 12 from the [REDACTED] logs, not because engineers purposely implemented an Incognito-detection bit
 13 in them. *Id.* ¶ 7.

14 2. [REDACTED] Logs

15 Google uses the [REDACTED]” logs at issue to test the functionality of an ad-serving
 16 framework called “Turtledove,” which is a publicly documented technology Google has proposed
 17 to enable remarketing and targeted advertisements without the use of third-party cookies. Kahlon
 18 Decl. ¶¶ 4–5; *see also id.* Exs. A, B, C. [REDACTED] logs [REDACTED]
 19 [REDACTED]
 20 [REDACTED]. *Id.* ¶ 5.

21 No new user data is written to these [REDACTED] logs. All event-level browsing data in those
 22 logs, including the “maybe_chrome_incognito” field, is duplicative of [REDACTED] log data. *Id.* ¶ 6;
 23 *see also* 6/14 Šrámek Decl. ¶ 7. None of the other information recorded in these [REDACTED] logs reflects
 24 actual user data. *Id.* Like the [REDACTED] logs, these [REDACTED] logs contain the “maybe_chrome_incognito”
 25 [REDACTED]

26 ³ [REDACTED] logs are called [REDACTED] logs because they allow operators to set experiments to run
 27 during low-traffic times, when Google’s systems have greater processing capacity available. Liu Decl. ¶ 6;
see also id. Ex. A.

28 ⁴ Google uses the term “user data” herein to refer to data generated by external users, in contrast to data
 generated by Google personnel conducting experiments using Google’s systems.

1 field only because they are automatically populated with copies of all fields from the [REDACTED]
 2 logs. Kahlon Decl. ¶ 7. As with the [REDACTED] logs, the “maybe_chrome_incognito” field in these [REDACTED]
 3 logs has not been used to identify or analyze Incognito browsing. *Id.* ¶ 8.

4 3. [REDACTED] Logs

5 [REDACTED] of the June Logs are [REDACTED] logs,” which store data from two or more other logs. Lee
 6 Decl. ¶¶ 2–3. Contrary to Plaintiffs’ accusation, *see* Dkt. 655-1 at 1, [REDACTED]
 7 [REDACTED]
 8 [REDACTED]
 9 [REDACTED], *see* Lee Decl. ¶¶ 4, 9, 10, 14, 15; Panferov Decl. ¶ 3; Psounis Decl. ¶¶ 17–21.
 10 Moreover, Google does not use the “maybe_chrome_incognito” bit in these logs to identify or
 11 analyze Incognito browsing, and the bit is present in those logs only because the [REDACTED] logs contain
 12 [REDACTED]. Lee Decl. ¶¶ 13. As described further below, none of the
 13 data stored in these logs is accretive.

14 [REDACTED] This log contains records from [REDACTED]
 15 logs: [REDACTED]
 16 [REDACTED], each of which contains only unauthenticated data. Lee Decl. ¶ 4.
 17 The log combines these records so that ads systems can access fields from across those input logs
 18 without reading multiple separate data sources. *Id.* Like all [REDACTED] logs, [REDACTED]
 19 [REDACTED]
 20 [REDACTED]
 21 [REDACTED]. Lee Decl. ¶¶ 4, 13.

22 [REDACTED]
 23 [REDACTED]. These
 24 [REDACTED] logs [REDACTED] as described in the Lee declaration. *Id.* ¶¶ 5–8.
 25 Each of the logs contributing to these [REDACTED] logs contains records keyed only to authenticated
 26 identifiers. *Id.* ¶ 6–8. Like [REDACTED], these [REDACTED] logs combine
 27 records so that ads systems can read fields spread across multiple logs efficiently from a single
 28

1 log. *Id.* [REDACTED]
 2 [REDACTED]. *Id.* ¶ 9.
 3 [REDACTED]. This log contains records from [REDACTED] logs
 4 containing only unauthenticated data [REDACTED]
 5 [REDACTED]. *Id.* ¶ 10. The log also contains [REDACTED]
 6 [REDACTED]
 7 [REDACTED] [REDACTED] [REDACTED]). *Id.*
 8 Although this log contains some records from [REDACTED] logs and other records from unauthenticated
 9 logs, the coding of the log prohibits it from ever [REDACTED]
 10 [REDACTED]. *See id.*; Panferov Decl. ¶ 3–5; Psounis Decl. ¶¶ 17–21.
 11 The coding of the log instructs it [REDACTED]
 12 [REDACTED]. Panferov Decl. ¶ 3; Psounis
 13 Decl. ¶¶ 12–17. Google will make the source code file substantiating this position, relevant portions
 14 of which are discussed in the Panferov and Psounis Declarations, available for Plaintiffs’ review
 15 pursuant to the terms of the Protective Order.

16 Google previously disclosed all [REDACTED] logs that contribute data to [REDACTED]
 17 [REDACTED]. *See* 5/31 Šrámek Decl.; 6/14 Šrámek Decl. ¶ 13. The log
 18 documentation for [REDACTED]
 19 [REDACTED] [REDACTED]
 20 [REDACTED]
 21 [REDACTED]. Lee Decl. ¶¶ 12–13; *id.* Ex. A. The log therefore contains no accretive information.

22 4. [REDACTED] Logs

23 [REDACTED] of the remaining logs at issue are “[REDACTED]” logs, which either [REDACTED]
 24 [REDACTED] containing maybe_chrome_incognito (all of which Google has disclosed) with information
 25 indicating that [REDACTED]
 26 [REDACTED]. *Id.* ¶¶ 16–17. These logs record neither event-level user data nor Incognito-detection fields
 27 beyond the data found in their underlying logs. *Id.* ¶ 20. Nor do they use Incognito-detection fields
 28 to identify or analyze Incognito browsing. *Id.* ¶ 21. Like the [REDACTED] logs discussed above, [REDACTED]

1 logs contain the “maybe_chrome_incognito” bit only because they contain [REDACTED]
 2 [REDACTED]. *Id.* ¶ 19. Therefore, [REDACTED] logs are also non-accretive.

3 5. [REDACTED] Logs

4 [REDACTED] more of the logs at issue are [REDACTED] logs, which record traffic data
 5 involving Google ads served via non-Google exchanges. Maki Decl. ¶ 7. One of the logs, [REDACTED]
 6 [REDACTED] is an equivalent variant of [REDACTED], one of the [REDACTED]
 7 [REDACTED] logs Google previously disclosed. *Id.* The principal difference between this [REDACTED] log
 8 and its [REDACTED] equivalent is that while the [REDACTED] log records only [REDACTED]
 9 [REDACTED]
 10 [REDACTED]), the [REDACTED] log records only [REDACTED]
 11 [REDACTED]. *Id.* The other [REDACTED] logs record a partial sample
 12 of instances in which [REDACTED]
 13 [REDACTED]. *Id.* The term [REDACTED] in each
 14 of these logs’ names refers only to the fact that they record traffic in [REDACTED]
 15 [REDACTED] the logs themselves are not shared outside of Google. *Id.* ¶¶ 7–9.

16 The “maybe_chrome_incognito” bit in the [REDACTED] logs is not used to
 17 identify or analyze Incognito browsing. *Id.* ¶ 10. The only reason these logs contain the
 18 “maybe_chrome_incognito” field is that they draw on the same [REDACTED] proto
 19 used by the [REDACTED] logs. *Id.* ¶ 8. Because they share that proto, fields added to the [REDACTED]
 20 logs are automatically replicated into the [REDACTED] logs. *Id.* Since these logs also
 21 provide no additional evidence about the use of Incognito-detection bits, they, too, are non-accretive.

22 6. [REDACTED] Logs

23 The remaining [REDACTED] logs containing the “maybe_chrome_incognito” bit are “[REDACTED] logs,”
 24 which contain only [REDACTED] (who are expressly
 25 excluded from the class). *Id.* ¶ 3. [REDACTED] logs do not contain user data, in Incognito mode or otherwise.
 26 *Id.* Like the [REDACTED] logs, the only reason the [REDACTED] logs at issue contain the
 27 “maybe_chrome_incognito” field is that they draw on the [REDACTED] proto, which
 28 automatically replicates fields added to the [REDACTED] logs into the [REDACTED] logs—whether or not that

1 field is populated with data reflecting user browsing activity. *Id.* ¶ 4. None of these [REDACTED] logs use
 2 “maybe_chrome_incognito” to identify or analyze Incognito browsing. *Id.* ¶ 5.

3 7. [REDACTED] Log

4 The final log at issue is [REDACTED], an [REDACTED] log that contains the
 5 “is_chrome_non_incognito_mode” bit. Kuzniar Decl. ¶ 2. That log is designed to eventually replace
 6 the previously disclosed [REDACTED]. *Id.* ¶ 4. Both logs are
 7 intended to serve the same function—to help the [REDACTED] team [REDACTED]
 8 [REDACTED]
 9 [REDACTED]. *Id.*; *see also* Dkt. 527-4 at 13. As a result, all of the fields in [REDACTED]
 10 [REDACTED] including “is_chrome_non_incognito_mode,” were replicated in
 11 [REDACTED]. *Id.* The replacement has not yet occurred, and
 12 [REDACTED] is not yet fully operational. *Id.* ¶ 5. Rather, it records only a
 13 random set of approximately one percent of the events recorded in [REDACTED]
 14 [REDACTED] (and until November 24, 2022 recorded only a [REDACTED] of that). *Id.*

15 This [REDACTED] log has not been used for analysis of Incognito browsing. *Id.* ¶ 8. Indeed, this
 16 log did not begin recording data until after the [REDACTED] team stopped using Incognito-detection bits
 17 for any purpose. *Id.* ¶ 5; FFCL ¶ 132. Even if the log were relevant to Plaintiffs’ claims (and it is
 18 not), it contains no user identifiers. Kuzniar Decl. ¶ 6–7. In other words, none of the data in this log
 19 is connected to a user or even a browser instance by a GAIA, Zwieback, Biscotti, or other ID. *Id.* ¶
 20 6; *id.* Ex. A.

21 **III. ARGUMENT**

22 The Court ordered Google to substantiate two propositions: (i) that the June Logs do not
 23 “contain relevant data that should have been identified and produced during discovery” and (ii) that
 24 Google should not be sanctioned. Dkt. 784. The evidence confirms both. Google engineers did not
 25 purposely implement the Incognito-detection bits in the logs at issue, and the bits were not used in
 26 those logs to identify or analyze Incognito browsing. In many cases, the logs contain no user data at
 27 all. Accordingly, these logs contain no data material to Plaintiffs’ claims, and Google should not be
 28 sanctioned for not having uncovered the June Logs earlier. The Court has already sanctioned Google

1 for not disclosing the Incognito-detection bits and the logs in which they were implemented earlier
 2 in the case. Google’s inability to identify these other logs earlier was justified, caused no additional
 3 prejudice to Plaintiffs, and—at worst—is part and parcel of the same conduct the Court has already
 4 addressed in a 57-page order following extensive briefing and a full-day evidentiary hearing. No
 5 further sanctions are warranted.

6 **A. The June Logs Do Not Contain Accretive Information**

7 The Court has already sanctioned Google for failing to identify and disclose earlier the
 8 Incognito-detection bits and the logs in which they were implemented to measure aggregate
 9 Incognito usage. *See* FFCL at 13, 27–28, 36. The question now is whether the logs at issue contain
 10 accretive material information. As explained above, they do not. *See supra* section II(D). Automated
 11 happenstance introduced the relevant Incognito-detection bits into the June Logs, and even if they
 12 had been discovered and disclosed, demand for either their preservation or production would not
 13 have been proportional to the needs of the case under Rule 26. Although the logs at issue may be
 14 cumulative evidence of the Incognito-detection bits’ *existence*, they provide no new evidence about
 15 the bits’ use. As explained below, none of these additional logs could have helped Plaintiffs establish
 16 liability, calculate damages, or identify class members in any way not addressed already in the
 17 Court’s May 20 Order. *See infra* section III(C)(1).

18 **B. Google Should Not Be Further Sanctioned**

19 A Court may sanction a party for discovery misconduct under either Federal Rule 37 or its
 20 inherent authority. *See Luxul Tech. Inc. v. NectarLux, LLC*, 2016 WL 3345464, at *4 (N.D. Cal.
 21 June 16, 2016). “Where the conduct for which sanctions are sought is not in violation of a specific
 22 discovery order governed by Rule 37, the district court must rely on its ‘inherent authority’ to impose
 23 sanctions.” *Id.* No sanctions are warranted on either basis. First, because the June Logs are not
 24 accretive, *see supra* sections II(D) & III(A), Google’s failure to disclose them during discovery is
 25 not a new violation of a discovery order. Second, because Google has at all times acted in good
 26 faith, sanctions under the Court’s inherent power are also unwarranted.

1 **1. Google Has Not Further Violated the Court’s Discovery Orders**

2 Discovery sanctions under Rule 37(b) are available only where a party has violated a
3 discovery order, *see Unigard Sec. Ins. Co. v. Lakewood Eng. & Mfg. Corp.*, 982 F.2d 363, 368 (9th
4 Cir. 1992), but Google has committed no new violations meriting further sanctions. The Court
5 sanctioned Google after finding that “not disclos[ing] to Plaintiffs, the Court, or the Special Master
6 . . . logs containing the maybe_chrome_incognito bit [or] . . . the is_chrome_incognito and
7 is_chrome_non_incognito bits” violated its November 12, 2021 order requiring a declaration that
8 Google had provided a list of data sources relevant to Plaintiffs’ claims (Dkt. 331).⁵ FFCL at 36.
9 Google’s failure to identify the June Logs is not a separate violation of that order. Although the June
10 Logs contain Incognito-detection bits, they reveal no information material to Plaintiffs’ claims
11 beyond that contained in the previously disclosed logs addressed in the Court’s May 20 order. *See*
12 *supra* section II(D); *infra* section III(C)(1). Thus, even if the Court were to find that Google’s
13 inability to identify and disclose the June Logs earlier constitutes misconduct, that failure would be
14 part and parcel of the precise conduct—failure to disclose logs containing Incognito-detection bits—
15 for which the Court already sanctioned Google.

16 **2. Google’s Good-Faith Conduct Does Not Warrant Sanctions Under the**
17 **Court’s Inherent Power**

18 Courts may sanction parties under their inherent authority only where that party has acted in
19 bad faith. *See* FFCL at 47 (citing *Chambers v. NASCO, Inc.*, 501 U.S. 32, 45–48 (1991); *Goodyear*
20 *Tire & Rubber Co. v. Haeger*, 137 S. Ct. 1178, 1186 (2017)). This requirement may be met only by
21 a showing of “willful misconduct, or recklessness combined with ‘frivolousness, harassment, or an
22 improper purpose.’” *Id.* (quoting *Fink v. Gomez*, 239 F.3d 989, 993–94 (9th Cir. 2001)). There has
23 been no such misconduct here.

24 The Court previously considered Google’s failure to identify the Incognito-detection bits
25 (and the logs in which they were implemented) despite its investigation into the “logs and other
26 sources that contained event-level user data . . . relevant to the products and claims at issue,” Dkt.

27 _____
28 ⁵ The Court also reiterated its November 12, 2022 determination that Google had violated two prior orders
(Dkt. 147-1, Dkt. 273) based on earlier misconduct. FFCL at 35.

1 527-14 (“4/1/22 Golueke Decl.”) ¶ 10, and held that (i) Google should have included the undisclosed
 2 logs containing the Incognito-detection bits in its disclosures to Plaintiffs, FFCL at 21, but (ii) there
 3 had been no showing that “Google’s failures in these regards resulted from either bad faith or
 4 recklessness with an improper purpose,” *id.* at 48.

5 The same logic applies doubly here. Google’s investigation to identify relevant data sources
 6 relied on “discussions with product managers and engineers who work directly on the products and
 7 the topics related to Plaintiffs’ claims,” 4/1/22 Golueke Decl. ¶ 10, and could not reasonably have
 8 revealed the existence of the June Logs because they (i) were not used for Incognito-specific
 9 analysis, and (ii) contained Incognito-detection bits due only to automatic duplication. Once Google
 10 learned of the June Logs, it disclosed them to Plaintiffs immediately. *See* 6/14 Šrámek Decl.

11 **C. None of the Sanctions Plaintiffs Request Is Warranted Here**

12 Even if the Court were to find that Google’s conduct fell short of its obligations, that finding
 13 would not merit the extreme sanctions Plaintiffs seek. Contrary to Plaintiffs’ arguments, Google’s
 14 failure to identify and disclose the June Logs earlier has caused no prejudice at all, let alone new
 15 prejudice the Court has not already addressed in the May 20, 2022 order. None of the harsh sanctions
 16 Plaintiffs request is warranted.

17 **1. Plaintiffs Have Not Been Further Prejudiced**

18 The June Logs do not contain material accretive data. Therefore, even if they had been
 19 disclosed earlier, they would not have given Plaintiffs additional information material to liability,
 20 damages, or class certification.

21 **a. The June Logs Would Not Have Put Plaintiffs in a Better** 22 **Position to Argue Google’s Liability**

23 Because the June Logs establish nothing new about the existence or use of the Incognito-
 24 detection bits, their earlier disclosure would not have helped Plaintiffs prove any of their causes of
 25 action. Plaintiffs’ only argument that the June Logs bear on Google’s liability is that they
 26 purportedly “contain unique information about how Google uses private browsing activity,” Dkt.
 27 655-1 at 3, but the logs do no such thing. Plaintiffs erroneously conflate the presence of the
 28 Incognito-detection bits with the “use[] [of] private browsing activity.” As shown above, however,

1 the “maybe_chrome_incognito” bit is included in these logs as an artifact of Google’s backend
 2 infrastructure—not because Google used the bits in these logs to analyze private browsing activity.
 3 Declarant after declarant confirms that they know of no use of the Incognito-detection bits to identify
 4 or analyze Incognito browsing in *any* of these logs. *See supra* section II(D). Nearly [REDACTED] of those
 5 logs contain [REDACTED]. *See supra* section II(D)(6). Of the remaining logs that do [REDACTED]
 6 [REDACTED], that data is largely taken directly from logs that were disclosed to Plaintiffs (and the Court)
 7 in November 2021 and March 2022, *before* the Court ruled on Plaintiffs’ last sanctions motion. *See*
 8 *supra* section II(D); *see also* Dkt. 337–3; Dkt. 527–6 ¶ 55.

9 To the extent Plaintiffs’ claim is merely that the logs at issue show that Google leverages
 10 private-browsing data to support its advertising services, *see* Dkt. 655-1 at 7 (arguing that “Google
 11 was unjustly enriched by its collection and use of private browsing data”), that is not new either.
 12 Google acknowledged more than two years ago in written discovery that it uses private browsing
 13 data for the same purposes as other pseudonymous data.⁶ Indeed, because Google cannot reliably
 14 distinguish between private and non-private browsing activity—a prerequisite to excluding private
 15 browsing data from any given use—Google treats and uses such data the same.⁷ *See, e.g.*, Dkt. 527-
 16 4 at 8 (summarizing Google’s argument that bits based on the X-Client-Data header cannot identify
 17 event-level private browsing).

18 Plaintiffs argue that some logs at issue demonstrate that Google links logged-out users’
 19 private browsing data to authenticated (signed-in) data. Dkt. 655-1 at 7. Plaintiffs’ speculative
 20 assertion, based only on the fact that Google maintains a log that contains authenticated and
 21 unauthenticated records, is wrong. *See infra* section III(C)(2)(b). Though [REDACTED] of the [REDACTED]

22 _____
 23 ⁶ *See, e.g.*, Trebicka Decl. Ex. 1 at 3–4 (Resp. to Plf.’s RFA No. 2) (“Google code provided to third party
 24 websites for the purpose of [transmitting data to Google] is not designed to differentiate between private
 25 browsing/Incognito modes and other browsing modes.”); *id.* at 6–7 (Resp. to Plf.’s RFA No. 7) (“[W]hen a
 26 user is not signed into his or her Google account . . . Google may still receive data from its services—
 27 including from users in Incognito mode . . . [and] may use the data associated with cookies to personalize
 advertisements displayed to the user.”); *id.* at 9–10 (Response to Plf.’s RFA No. 11) (“Google . . . has earned
 revenue from advertising shown to users visiting websites that use Google’s advertising services, and . . .
 depending on the user’s settings and plug-ins, Google may have been able to display ads using data Google
 received while a user was in Incognito mode.”).

28 ⁷ Google’s equal treatment of pseudonymous data from private and non-private browsing aligns with
 industry standards. *See* Dkt. 659-3 at 24 n.32.

1 Logs” at issue stores some records [REDACTED]
 2 [REDACTED], that log is coded [REDACTED]
 3 [REDACTED], cannot be used to identify private browsing users, and in
 4 any case contains only data from previously disclosed logs. Lee Decl. ¶ 10; Panferov Decl. ¶¶ 3–5;
 5 Psounis Decl. ¶¶ 17–21.

6 That the logs at issue contain no accretive information material to Plaintiffs’ seven causes
 7 of action is unsurprising. Plaintiffs’ prior arguments concerning the existence and use of these bits
 8 have never focused on liability, and nothing about the logs at issue here makes them any more
 9 relevant to Plaintiffs’ causes of action than those at issue in Plaintiffs’ prior motion. To the contrary,
 10 because the Incognito-detection bits in these logs have not been used for Incognito-related
 11 analysis—or for any other purpose—the logs have no material relevance to Plaintiffs’ claims at all.
 12 See Dkt. 655-1 at 2 (asserting that the logs are relevant to the extent they demonstrate “tracking
 13 private browsing . . . and using that data for important business purposes,” which they do not).

14 **b. The June Logs Have No Bearing On Plaintiffs’ Alleged Damages**

15 Plaintiffs’ damages model relies on neither the Incognito-detection bits nor any other
 16 information they could supplement using the June Logs. Plaintiffs’ damages expert Michael
 17 Lasinski proposes two methodologies to calculate Plaintiffs’ alleged restitution and unjust
 18 enrichment damages: First, to calculate total class-wide restitution damages, Lasinski purports to
 19 multiply the number of unique browser instances that browsed in private browsing modes during
 20 each month of the class period by the \$3 per-device, per-month rate that Mr. Lasinski claims is the
 21 measure of restitution for Plaintiffs’ data. Dkt. 608-9 (“Lasinski Rep.”) ¶¶ 183–184. To arrive at his
 22 total damages estimate of \$9.1 billion, Mr. Lasinski estimates the number of monthly, unique,
 23 private browsing instances using UMA data Google produced. *Id.* This calculation does not rely on
 24 either the Incognito-detection bits or any log containing them.

25 Second, Mr. Lasinski purports to calculate unjust enrichment damages using a top-down
 26 approach based on Google’s U.S. revenues from Display Ads, Search Ads, and YouTube Ads in
 27 three scenarios. *Id.* ¶¶ 133–136. To estimate these values, Mr. Lasinski purports to use the inputs of
 28 Google’s internal [REDACTED] study, which [REDACTED]

1 [REDACTED] in Chrome. *Id.* ¶¶ 34–39. His calculations for unjust enrichment,
 2 which range from \$567.4 million to \$3.87 billion, *id.* ¶¶ 133–136, rely only on the [REDACTED]
 3 study and Google’s financial reporting. He does not rely on log data of any kind. Thus, the logs at
 4 issue would have had no effect on these calculations.

5 Plaintiffs also cannot genuinely claim that they would have used logs containing Incognito-
 6 detection bits to estimate damages had such logs been available. When Plaintiffs prepared and
 7 served Mr. Lasinski’s expert report in late April 2022, they knew about the Incognito dashboard,
 8 the three Incognito-detection bits, and [REDACTED] logs that contained them. They also knew that
 9 “maybe_chrome_incognito” was developed to support the [REDACTED] study on which Mr.
 10 Lasinski bases his unjust-enrichment damages model. *See* FFCL at 5. Plaintiffs still found the logs
 11 in which Incognito-detection bits were implemented unnecessary for their damages analysis. The
 12 June Logs (in which the Incognito-detection bits were not purposefully implemented) are even less
 13 relevant to those calculations.

14 **c. The June Logs Provide No New Information Concerning**
 15 **Plaintiffs’ Ability to Identify Class Members or Entitlement to**
 16 **Class Certification**

17 To date, Plaintiffs’ arguments about the Incognito-detection bits can be boiled down to the
 18 (erroneous) claim that “[w]hile Google was repeatedly representing to this Court that private
 19 browsing users cannot be identified, [Google engineers] were in fact developing (and eventually
 20 implemented) a tool designed to do precisely that” Dkt. 429-1 at 5. The question of whether
 21 these bits have any value for identifying Plaintiffs’ class has already been litigated extensively
 22 before this Court, *see* FFCL at 25, and nothing about the logs now at issue changes that state of play.

23 As the Court has recognized, the “reliability of using the Incognito-detection bits to identify
 24 Incognito traffic, let alone specific Incognito users, is in dispute.” FFCL at 25. Ample evidence
 25 shows that the Incognito-detection bits are not a reliable means of identifying Incognito traffic, much
 26 less specific Incognito users. *See, e.g.,* FFCL at 25; *see also* Berntson June 16, 2021 30(b)(6) Tr.
 27 373:17–376:13 (Trebicka Decl. Ex. 2); Dkt. 659-10 (“Psounis Class Cert. Rep.”) ¶¶ 142–145.
 28 Plaintiffs have argued that the bits can reliably detect Incognito users, *see* Dkt. 535-17, but the

1 existence of more logs containing the same contested bits provides no additional support for that
 2 claim. That is especially so given the logs at issue incorporated the Incognito-detection bits only by
 3 way of an automated process, and not because Google engineers intentionally included them. *See*
 4 *supra* section II(D).

5 Nor are the June Logs material to whether Plaintiffs’ claims are amenable to resolution on a
 6 classwide basis. For example, none of those logs shows whether putative class members were
 7 exposed to public information and disclosures that would support Google’s implied consent defense,
 8 Dkt. 659-3 (Google’s Class Cert. Opp.) at 12–13, or whether class members drew uniform
 9 inferences from Google’s disclosures about Incognito mode, *id.* at 7–9.

10 Indeed, Plaintiffs moved for class certification one week *after* receiving the June 14, 2022
 11 declaration identifying the logs at issue here. *See* Dkt. 609. Plaintiffs did not seek an extension; nor
 12 did they suggest in their motion (or at the October 11, 2022 class certification hearing) that the June
 13 Logs might bear on issues relevant to class certification. None of that is surprising: Plaintiffs have
 14 unequivocally maintained that they need not rely on *any* log data for class certification. *See* May 3,
 15 2022 Hr’g Tr. 13:6–8 (Ms. Bonn: “I don’t think Plaintiffs affirmatively, for our class certification
 16 motion, intend to rely on sampled data, or frankly, other data.”). Plaintiffs’ complaint in their
 17 supplemental sanctions motion that “Plaintiffs were unable to address these logs in their class
 18 certification motion,” Dkt. 655-1 at 4, is thus an empty one.

19 **d. The June Logs Would Not Have Further Changed the Course of**
 20 **Discovery**

21 In its May 20, 2022 order, the Court found that “[t]he course of discovery may have been
 22 different, more focused, or focused on different issues had Google complied with its discovery
 23 obligations,” and that Google’s noncompliance “prevented Plaintiffs from fully exploring and
 24 testing the ability to link Incognito traffic to class members’ . . . Google Account data.” FFCL at 31.
 25 Because the June Logs reveal nothing new about the existence or use of the Incognito-detection bits,
 26 their earlier disclosure would not have further focused the discovery process or helped Plaintiffs test
 27 Google’s ability to link Incognito traffic to class members.
 28

1 **2. Plaintiffs’ Requested Preclusion Sanctions Are Unwarranted and**
 2 **Unnecessary**

3 “[O]n the menu of sanctions that a court may select from in applying Rule 37, preclusion of
 4 evidence is among the most severe.” *True Health Chiropractic Inc. v. McKesson Corp.*, 2015 WL
 5 5341592, at *6 (N.D. Cal. Sept. 12, 2015) (quoting *Network Appliance, Inc. v. Bluearc Corp.*, 2005
 6 WL 1513099, at *3 (N.D. Cal. June 27, 2005)). Issue preclusion sanctions are also reserved for
 7 discovery abuse “so extreme and prejudicial that no lesser remedy will cure the harm.” *Synapsis,*
 8 *LLC v. Evergreen Data Sys., Inc.*, 2006 WL 2884413, at *1 (N.D. Cal. Oct. 10, 2006). As a result,
 9 preclusion sanctions are “rarely impose[d].” *Natural-Immunogenics Corp. v. Newport Tr. Grp.*,
 10 2016 WL 11520757, at *6 (C.D. Cal. June 16, 2016).

11 Moreover, where the proposed sanction would effectively dispose of a party’s claim or
 12 defense, a Court may grant that sanction only upon an express finding of “willfulness, fault, or bad
 13 faith.” *See R&R Sails, Inc. v. Ins. Co. of Pa.*, 673 F.3d 1240, 1247 (9th Cir. 2012) (claim-
 14 determinative sanctions inappropriate absent a finding of bad faith); *see also Nuance Comms., Inc.*
 15 *v. ABBYY Software House*, 2012 WL 5904709, at *2–3 (N.D. Cal. Nov. 26, 2012) (rejecting adverse
 16 jury instructions on “claim-determinative issues” where “Plaintiff has shown that it would prefer to
 17 obtain a directed verdict on some of its claims rather than prevailing on the merits.”).

18 There is no basis for such extreme and unusual sanctions here. Google has worked diligently
 19 and in good faith to provide Plaintiffs and the Court with detailed information about logs containing
 20 the Incognito-detection bits, and Plaintiffs have faced no prejudice—beyond what the Court has
 21 already cured—from Google’s timing in doing so.

22 **a. Excluding Reliance on Messrs. Šrámek and Harren**

23 Plaintiffs argue that the Court should preclude Google from offering or relying on any
 24 testimony from Martin Šrámek and Matt Harren “[c]onsistent with the relief previously granted by
 25 the Court.” Dkt. 655-1 at 5. But nothing in the Court’s prior order supports this preclusive sanction.
 26 The Court’s May 20, 2020 order precluded testimony by four Google engineers *who developed and*
 27 *implemented* the Incognito-detection bits. *See* FFCL at 4–6, 45. Messrs. Šrámek and Harren, by
 28 contrast, were assigned to investigate logs that may contain those bits—*after* the Court ruled on

1 Plaintiffs’ sanctions motion—in order to comply with the Court’s order. *See* Dkt. 614-2, 614-3.
 2 Thus, their knowledge became relevant only as a result of the Court’s order, not as a result of
 3 Plaintiffs’ claims.

4 **b. Precluding Argument on Joining Authenticated and**
 5 **Unauthenticated Data**

6 Plaintiffs also ask the Court to preclude Google “from arguing that it does not join Incognito
 7 browsing data to authenticated data,” 655-7, because, they claim, the logs at issue show Google
 8 “combine[s] private browsing data with authenticated data in a single log,” Dkt. 655-1 at 1. This
 9 proposed sanction is particularly extreme, unfair, and prejudicial because it would effectively
 10 preclude Google from asserting a key defense: that Incognito *is* private because it prevents Google
 11 from identifying the user (unless he/she signs in to a Google Account, which would exclude them
 12 from the class). In any event, this sanction is without basis here because, as demonstrated above,
 13 Plaintiffs’ factual premise is wrong.

14 The extensive factual record confirms that Google’s log data usage policies expressly
 15 prohibit joining authenticated data (data associated with a Google Account) with unauthenticated
 16 data (such as data Google receives when a user is in private browsing and not signed into a Google
 17 Account), *see, e.g.*, Dkt. 695-7 at -456; Dkt. 695-8, at -039, and that Google complies with these
 18 policies,⁸ *see, e.g.*, Trebicka Decl. Ex. 2 (Berntson 6/16/21 30(b)(6) Tr. 199:1–5) (“Google has a set
 19 of . . . policies that are meant to prevent reidentifiability, prevent joining of sort of sensitive IDs in
 20 terms of, say, signed in and signed out.”); Lee Decl. ¶ 15 (“I am not aware of any logs at Google
 21 that join records of authenticated information with records of unauthenticated information, nor have
 22 I ever been aware of any such logs at any time during the course of my [over 10 years of]
 23 employment at Google.”); Psounis Class Cert. Rep. ¶¶ 100–108; Dkt. 659-11 (Schwartz Class Cert.
 24 Rep.) ¶¶ 87–93. Indeed, after years of extensive discovery, Plaintiffs’ technical and privacy experts
 25 have been forced to admit they cannot identify a single instance in which Google linked
 26

27 ⁸ Even former Google employee Rory McClelland—whose attorneys fees and travel costs in this litigation
 28 were paid by Plaintiffs—agreed. *See* Trebicka Decl. Ex. 3, McClelland 2/18/22 Tr. at 228:23–229:9; 278:5–
 23.

1 unauthenticated private browsing activity data to a user or her account, or to her signed-in activity.
 2 Dkt. 659-3 at 11 (citing *Schneier* 7/18/22 Tr. 112:15–20); Dkt. 666-2 at Ex. 32, 136:18–24 (“Q. ...
 3 you haven’t seen any evidence that Google’s actually done that [i.e., join authenticated and
 4 unauthenticated data]? A. No.”). None of the June Logs indicates otherwise. *See supra* section II(D).
 5 [REDACTED]
 6 [REDACTED]
 7 [REDACTED]. *See supra* section II(D)(3).

8 Plaintiffs’ proposed sanction is also inappropriate because they have suffered no prejudice
 9 the Court has not already addressed. *See supra* section III(C)(1). The evidence submitted with this
 10 briefing conclusively establishes that, had Plaintiffs conducted further discovery on the [REDACTED] logs,
 11 they would have learned only that Google does not join authenticated and unauthenticated data. *See*
 12 Lee Decl. ¶¶ 4, 9; Panferov Decl. ¶ 3; Psounis Decl. ¶¶ 17–21. No preclusive sanction is warranted.

13 c. Other Proposed Preclusion Sanctions

14 Plaintiffs also ask the Court to preclude Google from arguing that (i) “it does not use
 15 Incognito browsing data to ‘perform analysis and modeling to predict ad revenues’”; (ii) “it does
 16 not use Incognito browsing data for ‘ads related to third-party exchanges’”; and (iii) “it has not made
 17 Incognito browsing data available for other business purposes.” Dkt. 655-7.

18 These sanctions, too, are unwarranted. Google has long been transparent that data Google
 19 receives from Incognito browsing sessions is used the same way as non-Incognito data because
 20 Google has no reliable means of distinguishing Incognito and non-Incognito browsing data. *See*
 21 *supra* section III(C)(1)(a). Thus, Google could not make the arguments Plaintiffs (bizarrely) ask the
 22 Court to preclude without contradicting its own long-held position and sworn written discovery
 23 responses. Though Google has no intention of making such arguments, the Court should not
 24 preclude them as a sanction where, as here, no sanction is warranted.

25 3. Further Adverse Jury Instructions Are Unwarranted

26 Jury instructions are an extreme remedy that should be imposed only in the most serious and
 27 prejudicial circumstances. *See, e.g., Apple Inc. v. Samsung Elecs. Co.*, 888 F. Supp. 2d 976, 994
 28 (N.D. Cal. 2012). Adverse instructions to address alleged spoliation should be particularly limited.

Under Rule 37(e), “[i]f a court finds that the loss of [electronically stored] information has prejudiced the moving party, it may order ‘measures no greater than necessary to cure the prejudice.’” *Best Label Co. v. Custom Label & Decal, LLC*, 2022 WL 1525301, at *2 (N.D. Cal. May 13, 2022) (quoting Fed. R. Civ. P. 37(e)(1)). These measures may include an adverse jury instruction only if the court further finds that the nonmoving party “acted with the intent to deprive another party of the information’s use in the litigation.” *Id.* (citing Fed. R. Civ. P. 37(e)(2)). “[E]ven gross negligence . . . in failing to retain relevant evidence is not sufficient to support an adverse inference under Rule 37(e)(2).” *Meta Platforms, Inc. v. BrandTotal Ltd.*, 2022 WL 1990225, at *6 (N.D. Cal. June 6, 2022). No adverse instruction is warranted here.

Rule 37(e) forecloses an adverse instruction in connection with Plaintiffs’ allegations of spoliation because—in addition to the lack of prejudice, *see supra* section III(C)(1)—Google had no “intent to deprive” Plaintiffs of the information set forth in the June 14 declaration. To the contrary, Google’s thorough investigations and subsequent disclosures demonstrate Google’s intent to be completely transparent. Plaintiffs may argue (wrongly) that Google should have identified and preserved the logs at issue sooner, but that argument, which alleges negligence, not intentional conduct, cannot support an adverse instruction. *See Meta Platforms*, 2022 WL 1990225, at *6.

Nor is any further instruction warranted under Rule 37(b)(2)(A). The Court has already found that, should the Incognito-detection bits become relevant to an issue before the jury, an appropriate instruction would be that “Google failed to disclose relevant data sources reflecting the use of the Incognito-detection bits.” FFCL at 42. Plaintiffs’ accusations of additional misconduct are fully encompassed by that sanction. Thus, even if Plaintiffs’ claims of further prejudice had merit (and they do not), those claims would not justify any additional adverse jury instruction.

4. Shifting All Special Master Fees to Google Is Inappropriate Here

Federal Rule of Civil Procedure 37(b)(2) “provides for the award of reasonable expenses and attorney’s fees ‘caused by the failure’ to obey a court order to provide or permit discovery.” *Toth v. Trans World Airlines, Inc.*, 862 F.2d 1381, 1385-86 (9th Cir. 1988). “Expenses incurred outside of this particular context are not provided for in Rule 37(b)(2).” *Id.* Courts generally interpret the fees traceable to the failure as those incurred in bringing the sanctions motion

1 itself. *See, e.g., First Fin. Sec., Inc., v. Freedom Equity Grp., LLC*, 2016 WL 5870218, at *7 (N.D.
2 Cal. Oct. 7, 2016).

3 The standard to shift the costs of the Special Master process onto Google is not met
4 here. As the Court recognized in its May 20, 2022 order, “the identification and production of clearly
5 relevant data relating to Incognito-detection bits [is] but a small part of a complex process spanning
6 nearly a year of proceedings before the Special Master.” FFCL at 32. And as the Court further found,
7 “the reliability of” the bits contained in the June Logs “in identification of putative class members
8 remains the subject of strenuous debate” and “it is neither possible nor practicable to quantify either
9 the temporal or monetary impact of these particular issues on the greater process before [the] Special
10 Master.” *Id.* The logs at issue provide no additional information that would have obviated the special
11 master process (or a portion of it). Accordingly, Rule 37 does not authorize the relief Plaintiffs seek.

12 **IV. CONCLUSION**

13 For the foregoing reasons, Google respectfully submits that no further sanction is warranted.
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 DATED: November 30, 2022

QUINN EMANUEL URQUHART &
SULLIVAN, LLP

By: /s/ Andrew H. Schapiro

Andrew H. Schapiro (admitted *pro hac vice*)

andrewschapiro@quinnemanuel.com

Teuta Fani (admitted *pro hac vice*)

teutafani@quinnemanuel.com

Joseph H. Margolies (admitted *pro hac vice*)

josephmargolies@quinnemanuel.com

191 N. Wacker Drive, Suite 2700

Chicago, IL 60606

Telephone: (312) 705-7400

Facsimile: (312) 705-7401

Stephen A. Broome (CA Bar No. 314605)

stephenbroome@quinnemanuel.com

Viola Trebicka (CA Bar No. 269526)

violatrebicka@quinnemanuel.com

Crystal Nix-Hines (CA Bar No. 326971)

crystalnixhines@quinnemanuel.com

Alyssa G. Olson (CA Bar No. 305705)

alyolson@quinnemanuel.com

865 S. Figueroa Street, 10th Floor

Los Angeles, CA 90017

Telephone: (213) 443-3000

Facsimile: (213) 443-3100

Diane M. Doolittle (CA Bar No. 142046)

dianedoolittle@quinnemanuel.com

Sara Jenkins (CA Bar No. 230097)

sarajenkins@quinnemanuel.com

555 Twin Dolphin Drive, 5th Floor

Redwood Shores, CA 94065

Telephone: (650) 801-5000

Facsimile: (650) 801-5100

Josef Ansorge (admitted *pro hac vice*)

josefansorge@quinnemanuel.com

Xi ("Tracy") Gao (CA Bar No. 326266)

tracygao@quinnemanuel.com

Carl Spilly (admitted *pro hac vice*)

carlspilly@quinnemanuel.com

1300 I. Street, N.W., Suite 900

Washington, D.C. 20005

Telephone: 202-538-8000

Facsimile: 202-538-8100

1 Jomaire A. Crawford (admitted *pro hac vice*)
2 jomairecrawford@quinnemanuel.com
3 51 Madison Avenue, 22nd Floor
4 New York, NY 10010
5 Telephone: (212) 849-7000
6 Facsimile: (212) 849-7100

7 Jonathan Tse (CA Bar No. 305468)
8 jonathantse@quinnemanuel.com
9 50 California Street, 22nd Floor
10 San Francisco, CA 94111
11 Telephone: (415) 875-6600
12 Facsimile: (415) 875-6700

13 *Attorneys for Defendant Google LLC*
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28